

REMARKS

This communication is responsive to the Office Action dated August 2, 2007 and received in this application. Claims 10-12, 22-24 and 43-45 have been amended and claims 1-24 and 35-46 remain pending in the application. These amendments add no new matter. Reconsideration of the pending claims is respectfully requested in light of these amendments and the following remarks.

Claims 1-9, 13-21 and 35-42 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,286,099 to Kramer ("Kramer") in view of U.S. Pat. No. 5,880,769 to Nemirofsky ("Nemirofsky"). This rejection is traversed.

Independent claim 1 recites: *[a]n authentication system, said authentication system comprising:*

a portable card terminal, including:

first identification information storage means having a first identification information stored therein for discriminating said portable card terminal, said first identification information comprising a portable card terminal identifier that uniquely identifies the portable card terminal,

operating means for inputting a second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on encryption key information, and

first communication means for communication with an authentication device, wherein said communication includes transmitting the first identification information to said authentication device and receiving said encryption key information from the authentication device in response to transmitting the first identification information;

said authentication device, provided independently of said portable card terminal for communication with said portable card terminal, the authentication device including:

second identification information storage means for storage of the first identification information and the second identification information therein,

encryption key information generating means for generating said encryption key information, wherein said encryption key information comprises a random number, and wherein said encryption key information is generated in response to receiving the first identification information from said portable terminal,

second communication means for communication with said portable card terminal, and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key information;

wherein said portable card terminal encrypts the second identification information input from said operating means, based on said encryption key information received from said authentication device, the so-encrypted second identification information is transmitted through said first communication means to said authentication device; and

wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key information to perform the authentication.

Applicant appreciates the withdrawal of the previously relied-upon grounds of rejection, but submits that the new grounds of rejection remain deficient with regard to the claimed invention, and requests reconsideration and withdrawal of the new grounds of rejection.

Kramer merely appears to disclose that a session key may be generated and used to accommodate the encryption of communications between two devices. In this regard, Kramer does not appear to add anything beyond the previously relied-upon references that were cited for their disclosures of encryption techniques (*e.g.*, Schneier I and Schneier II, see previous responses and Appeal Brief).

Applicant's claimed invention provides a technique for protecting unauthorized access to

private information in a situation where the user accesses information using a portable card terminal that communicates with an authentication system. Independent claim 1 recites authentication features involving the first identification information (*e.g.*, the portable card terminal ID), correlated generation of an encryption key, and encryption of second identification information input to the portable card terminal using the encryption key. Specifically, the claim recites authentication wherein (1) the “first identification information” (further recited as the portable card ID) is sent from the portable card terminal to the authentication device, (2) the authentication device generates the encryption key in response to receiving the first identification information, (3) the authentication device sends the so-generated encryption key back to the portable terminal device, and (4) the portable terminal device then uses the encryption key to encrypt second identification information input to the portable card terminal (*e.g.*, the PIN entered by the user) and sends this encrypted second identification information to the authentication device, which then performs authentication.

Nemirofsky discloses a smart card that stores account information for remote financial services. A connection with a financial institution is initiated through the smart card, and data is exchanged to carry out a fully automated transaction. A user may also be required to enter a PIN code that is associated with the smart card, for enhanced security. Nemirofsky makes no mention of encrypting the PIN code. In that sense, Nemirofsky appears to disclose a typical banking card type exchange, wherein the user enters the PIN code and that information allows the user to continue access to financial or other information. There is no mention of encrypting the PIN code even generally, let alone according to the specific exchange of information claimed by Applicant.

The Examiner has previously admitted that Nemirofsky does not disclose encrypting based upon an encryption key received from an authentication device. (Final Office Action dated 8/23/06, at p. 3). Applicant concurs with this conclusion. However, Applicant submits that this is a simplification of the deficiencies of Nemirofsky, as various claimed features are absent from that reference.

Nemirofsky discloses a smart card, and discloses that a PIN may be used in association with usage of the smart card, but makes no mention with regard to *any* encryption technique for

that PIN, let alone the particular sequence claimed by Applicant. In fact, the entirety of the above-described sequence of Applicant's claimed invention is absent from Nemirofsky. At best, Nemirofsky uses a PIN that is sent to the authentication device. There is no mention in the reference of (1) sending the "first identification information" (the portable card ID) from the portable card terminal to the authentication device, (2) having the authentication device generate the encryption key in response to receiving the first identification information, (3) having the authentication send the so-generated encryption key back to the portable terminal device, (4) then having the portable terminal device use the encryption key to encrypt second identification information that is input to the portable card terminal (*e.g.*, the PIN entered by the user) and send the encrypted second identification information to the authentication device, which finally performs authentication.

Kramer does not remedy the deficiencies of Nemirofsky. As noted by the Examiner, Kramer does not disclose a portable card terminal with operating means for inputting second identification information associated with the first identification information. The Examiner refers to FIGs. 4 and 6 and some related description in Kramer as purportedly disclosing all but the portable card terminal with operating means for inputting the second identification information. However, Applicant submits that more than just these claimed features are absent from Kramer, as Kramer does not appear to send the first identification information from the portable terminal to the authentication device, then have the authentication device generate an encryption key and send it to the portable terminal, and finally have the portable terminal device use the encryption key to encrypt the second identification information.

FIG. 5 appears to disclose a flow of messages between a "POI Device" 5000 and a Financial Institution 5100, wherein the POI device sends keys, and optionally a "Device Properties Descriptor" (DPD), to the FI, which then returns a public key back to the POI device. The POI device uses the public key of the FI to encrypt communications so that only the FI can decrypt them. In this scheme, the public key is the public key of the FI, and not a particular key that is generated and associated to the POI device based upon its first identification information. FIG. 6, and column 9, lines 35-48 appear to disclose a similar sequence, but with a session key sent in the permission message. There is clearly no description of the sequence of sending the

first identification information from the portable terminal to the authentication device, then having the authentication device generate an encryption key and send it to the portable terminal, and finally having the portable terminal device use the encryption key to encrypt the second identification information.

It is also noted that a proper motivation to combine the references in the offered fashion is absent. *Prima facie* obviousness of a claimed invention is established “only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references.” *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). There are three possible sources for a motivation to combine references: 1) the nature of the problem to be solved, 2) the teachings of the prior art, and 3) the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1358, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998).

Here, there is no express, implied or any kind of apparent motivation for the artisan to modify Kramer according to the teachings of Nemirofsky. As described above, there is no mention of encrypting the PIN code of Nemirofsky. Therefore, one would not look to specific techniques given that there is no general suggestion to even consider such a modification. Also, one first considering the teachings of Kramer would in no way be motivated to look to Nemirofsky. Kramer makes no mention of applying the disclosed techniques to situations where a portable card terminal interfaces with an authentication system, and makes no mention of the desirability of generating an encryption code based upon a card ID, or of encrypting a user-entered PIN code in the sequence claimed by Applicant. There is clearly no objectively reasonable reason that one would conclude that the artisan would be motivated to combine the relied upon references in the fashion envisioned (in hindsight) by the Examiner.

Regardless, Applicant submits that, even assuming for the sake of argument that motivation to combine the references is present, a *prima facie* case of obviousness remains absent. This is because even a combination of the references would still fail to yield various features of the claimed invention.

For reasons similar to those provided regarding claim 1, independent claims 13, 35 and

46 are also neither disclosed nor suggested by the relied upon references.

Dependent claims 2-9, 14-21 and 39-42 are neither disclosed nor suggested for their incorporation of the features respectively recited in the independent claims as described above. Moreover, the dependent claims include their own separately recited features that are neither disclosed nor suggested by the relied upon references.

With regard to claims 6, 18 and 39, the relied upon references clearly fail to disclose or suggest “wherein said portable card terminal includes a transient storage means in which the second identification information is stored transiently.”

With regard to claim 7, 19 and 40 the relied upon references clearly fail to disclose or suggest “wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable card terminal by said authentication device.”

With regard to claims 8, 20 and 41, the relied upon references clearly fail to disclose or suggest “wherein said second identification information stored in said transient storage means is erased every preset time interval.” Applicant objects to the taking of official notice regarding these features, and any prior official notice is not applicable as, even if it was taken, it was taken in the context of different grounds of rejection.

Finally, with regard to claims 9, 21 and 42, the relied upon references clearly fail to disclose or suggest “wherein said operating means in said portable card terminal includes means for erasing the second identification information stored in said transient storage means.”

Applicant respectfully requests reversal of the Examiner’s rejection of claims 1-9, 13-21 and 35-42 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky.

Claims 10-12, 22-24 and 43-46 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky, and further in view of U.S. Pat. No. 5,276,314 to Martino (“Martino”). This rejection is traversed.

Claims 10-12, 22-24 and 43-46 variously depend from the above-described independent claims and thus incorporate the features recited therein. Martino is relied upon for disclosure of

an identify verification system said to be resistant to compromise by observation of its use, and offers no disclosure with regard to the above-described features. Accordingly, the combination of Kramer, Nemirofsky and Martino would still fail to yield the features of Applicant's claimed invention, and a prima facie case of obviousness remains absent.

Additionally, claim 10 (and similarly claims 12 and 43) now recites: "... *wherein said operating means in said portable card terminal includes a plurality of input locations respectively used for indicating letters or numerical figures for inputting said second identification information, and wherein the input locations corresponding to individual ones of the letters or numerical figures are variable, such that individual ones of the letters or numerical figures are resident at one of the plurality of input locations when said second identification information is input a first time, and are resident at another of the plurality of input locations when said second identification information is input a second time.*" Prompting variance between first and second input times is not disclosed or suggested by Martino.

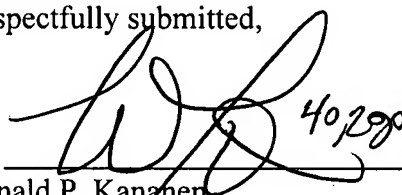
Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 10-12, 22-24 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over Kramer in view of Nemirofsky, and further in view of Martino.

In view of the foregoing arguments, all claims are believed to be in condition for allowance. If any further issues remain, the Examiner is invited to telephone the undersigned to resolve them.

This response is believed to be a complete response to the Office Action. However, Applicant reserves the right to set forth further arguments supporting the patentability of their claims, including the separate patentability of the dependent claims not explicitly addressed herein, in future papers. Further, for any instances in which the Examiner took Official Notice in the Office Action, Applicant expressly does not acquiesce to the taking of Official Notice, and respectfully request that the Examiner provide an affidavit to support the Official Notice taken in the next Office Action, as required by 37 CFR 1.104(d)(2) and MPEP § 2144.03.

Dated: November 1, 2007

Respectfully submitted,

By  40,290

Ronald P. Kananen

Registration No.: 24,104

Christopher M. Tobin

Registration No.: 40,290

Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC

Lion Building, 1233 20th Street, N.W., Suite 501

Washington, D.C. 20036

Tel: (202) 955-3750; Fax: (202) 955-3751

Customer No. 23353